



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/483,164	01/14/2000	Daniel Jay Thomsen	105.174US1	8029
21186	7590	09/13/2006	EXAMINER	
SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A. P.O. BOX 2938 MINNEAPOLIS, MN 55402				SIMITOSKI, MICHAEL J
ART UNIT		PAPER NUMBER		
2134				

DATE MAILED: 09/13/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/483,164	THOMSEN ET AL.
	Examiner	Art Unit
	Michael J. Simitoski	2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 18 May 2006.

2a) This action is FINAL. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-35 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 1-35 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on 18 May 2006 is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) All b) Some * c) None of:

- Certified copies of the priority documents have been received.
- Certified copies of the priority documents have been received in Application No. _____.
- Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)

2) Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) Notice of Informal Patent Application (PTO-152)

6) Other: _____.

DETAILED ACTION

1. The response of 5/18/2006 was received and considered.
2. Claims 1-35 are pending.

Response to Arguments

3. Applicant's arguments filed 5/18/2006 have been fully considered but they are not persuasive.
4. Applicant's response (§101 Rejections) suggests that claims 6 & 11 were amended to overcome the §101 rejections. However, as amended, claim 6 still recites a security system comprising only abstract ideas (layers), a user interface (software, *per se*) and a translator (software, *per se*). The limitation "for a computer network" does not limit the claim's scope to a machine or computers, as a computer network is a collection. Further, "within a model implemented on the computer network" further indicates that the semantic layers are just abstract ideas as they are within a "model". Similarly, claim 11 recites a system "for a computer network" and comprising a model "implemented on the computer network". It remains that the elements of the systems claimed in claims 6-13 are not tangibly embodied and do not fall within one of the four statutory classes of invention. Applicant's specification (p. 5) outlines various assertions towards tangible subject matter, for instance that "processing" or "computing" or "calculating" or "determining" or "displaying" or the like refer to the action and processes of a computer system, or similar electronic computing devices.... Applicant is encouraged to incorporate subject matter which tangibly embodies the systems of claims 6-13 to overcome the §101 rejection.

5. Applicant's response (§112 Rejections) argues that amendments have been made to clarify the §112 rejections. While the Examiner disagrees with reciting "a plurality of semantic layers" followed by "the two or more semantic layers", the Examiner considers this proper antecedent basis for the claim terminology "the two or more semantic layers". Further, Applicant's amendments have overcome the remaining §112 rejections.

6. Applicant's response (§102 Rejections) argues that the submitted affidavits establish the inapplicability of using the Thomsen references. However, the affidavits submitted are not sufficient.

a. Regarding the petition and evidence in contacting Jessica Bogle, Applicant is required to submit documentation regarding more than one attempt to contact the inventor at a known address. Applicant appears to have only attempted one contact at a known address.

b. Because the Thomsen reference is the work of three of the four inventors of the application, the Office needs to know the contribution of the fourth inventor who is not included as an author on the Thomsen article. The Office also requires a description of the claimed subject matter to which the fourth inventor contributed.

c. Applicant has submitted an affidavit to establish invention prior to October 1999, the date of "Napolean Network Application Policy Environment". However, evidence is required declaring what parts of the Thomsen article were invented prior to October 1999 and to what claims that subject matter applies. Further, Applicant must show in what time period reduction to practice occurred and must show diligence between the conception and reduction to practice. This information is similarly required to establish a

date of invention prior to December 1999, the date of “Role Based Access Control Framework for Network Enterprises”.

7. Applicant's response (p. 11, §3) argues that “Applicant is unable to find a teaching or suggestion in Sandhu that would lead one to encapsulate ‘security mechanism application specific information for each security mechanism’”. Sandhu discloses the following concepts: (1) Permissions are encapsulated into abilities (which can contain other abilities), and (2) abilities are assigned, with users, to roles (which can contain other roles). As Applicant describes, the present invention defines a security mechanism as something that “encapsulates security mechanism application specific information”. Sandhu defines a permission as “an approval of a particular mode of access to one or more objects”. Therefore, Sandhu discloses security mechanism application specific information because the permissions are application specific (they define precisely an object and an approval for accessing that object in an application) and they are security mechanisms because they define access rights.

8. Applicant's response (p. 11, §3) argues that “Applicant cannot find in Sandhu any teaching or suggestion of encapsulating key chains as keys and passing the key chain keys to another semantic layer.” Applicant further alleges that the Office Action reads UP-roles onto the semantic layers of the claims, but does not show that the UP-role of Sandhu does not teach or suggest the flexibility of passing the key chain keys to another semantic layer. However, Sandhu discloses permissions being combined into abilities (keys) and abilities combined with other abilities for form new abilities (key chains) and encapsulating key chains/abilities as keys/abilities and passing the key chain keys/abilities to another semantic layer (UP-roles) (p. 122, §5). Because UP-roles can contain other UP-roles (UP-roles), there exists another semantic

layer where UP-roles are encapsulated into a UP-role and exported (i.e. a first semantic layer containing UP-roles and a second semantic layer containing combined and encapsulated UP-roles from the first semantic layer) (p. 122, §5).

9. Applicant's response (p. 12, §103 Rejections) argues that the claims are allowable based on the insufficiency of the Sandhu reference. However, as described above, the rejections based on Sandhu are maintained.

Claim Rejections - 35 USC § 101

10. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

11. Claims 6-13 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The elements of the systems claimed in claims 6-13 are not tangibly embodied and do not fall within one of the four statutory classes of invention.

Claim Rejections - 35 USC § 102

12. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

13. Claims 1-3, 5-6 & 11-13 are rejected under 35 U.S.C. 102(a) as being anticipated by printed publication “Role Based Access Control Framework for Network Enterprises” by Thomsen, O’Brien and Bogle (**Thomsen**).

Regarding claim 1, Thomsen discloses encapsulating security mechanism application specific information for each security mechanism/methods (Fig. 1 & §2.4), wherein encapsulating includes forming a key for each security mechanism (Fig. 2 & §2.4), combining keys to form key chains (Figs. 1 & 2), encapsulating key chains as keys (for example “Doctor” and “Nurse”, Fig. 2) as keys (“Health Care Provider”, Fig. 2) and passing the key chain keys to another semantic layer (from application to enterprise) (§2.5), defining the security policy, wherein defining includes forming key chains from keys and associating users with key chains (§2.6-§2.7), translating the security policy (p. 7, last ¶2) and exporting the translated security policy to the security mechanisms (to CORBA using ADAGE (p. 8, ¶1) and enforcing the security policy via the security mechanisms/CORBA (p. 8, ¶1).

Regarding claim 2, Thomsen discloses a distributed computer network (§1.1).

Regarding claim 3, Thomsen discloses the security mechanisms being heterogeneous (p. 8, §3.2).

Regarding claim 5, Thomsen discloses defining the policy using a graphic user interface/NAPOLEAN policy tool (Fig. 4 & §3.1, “Specifying Policy”).

Regarding claim 6, Thomsen discloses a plurality of security mechanisms (§1.3), a plurality of semantic layers within a model implemented on the computer network (§2.5) wherein the two or more of the semantic layers include keys (primary physician, consulting physician) combinable into key chains (doctor) (§2.4), the key chains are able to be encapsulated as key chain keys (§2.4 and §2.6), and the key chain keys are exportable to another semantic layer/enterprise (§2.5-2.6), wherein each key encapsulates security mechanism application specific information (§1.3) for a security mechanism, a user interface for defining a security

policy as a function of keys received from a lower semantic layer (Fig. 5) and a translator for translating the security policy to the security mechanisms (§3.1).

Regarding claims 11 & 13, Thomsen discloses a model implemented on a computer network (§2.5), the model comprising semantic layers for defining different security policies and constraints for each type of user (Fig. 1), a tool for manipulating the model (§3), wherein the tool is configured to encapsulate security mechanism application specific information for each security mechanism, wherein encapsulating includes forming a key for each security mechanism (Fig. 2), combine keys (primary physician, consulting physician) to form key chains (doctor) (§2.4), encapsulate key chains as key chain keys within two or more semantic layers (§2.4 and §2.6), pass the key chain keys to other semantic layers/doctor to other semantic layers/enterprise (§2.5-2.6), form user key chains from the key chain keys (§2.6 & Fig. 4) and associate users with the user key chains (§2.6) and a translator for translating security policies from the model to the security mechanisms in one or more computer resources (§3.1).

Regarding claim 12, Thomsen discloses associating a constraint with a key (§2.3) where the constraint must be satisfied before access to a computer resource governed by the key chain is granted (§2.3 ¶1).

14. Claims 1-35 are rejected under 35 U.S.C. 102(a) as being anticipated by printed publication “Napoleon Network Application Policy Environment” by Thomsen, O’Brien and Payne (**Thomsen**). Thomsen discloses using an application layer, semantic layers and a local layer (Fig. 2 & §2), encapsulating keys into key chains, and exporting the key chains to the next layer (§2 & Fig. 2), combining methods into handles, handles into keys and keys into key chains

(Fig. 3), and adding constraints to the key chains at each layer (Fig. 4), assigning users to key chains (§2.3), using a user interface to manage the RBAC policy (§3) and translating the policy to the security mechanisms (§4).

15. Claims 1-4 & 32 rejected under 35 U.S.C. 102(a) as being anticipated by “The ARBAC97 Model for Role-Based Administration of Roles” by Sandhu et al. (**Sandhu**).

Regarding claim 1, 3 & 32, Sandhu discloses encapsulating security mechanism application specific information/permissions for each security mechanism/permission (p. 122, §5), wherein encapsulating includes forming a key/ability for each security mechanism/permission, combining keys/abilities to form key chains/abilities, encapsulating key chains/abilities as keys/abilities (p. 122, §5) and passing the key chain keys/abilities to another semantic layer/UP-Roles (p. 122, §5), defining the security policy/UP-Roles (p. 122, §5), wherein defining includes forming key chains from keys/abilities and associating users with key chains/abilities (p. 122, §5), translating the security policy/UP-Roles and exporting the translated security policy to the security mechanisms, and enforcing the security policy via the security mechanisms (p. 107, ¶5 & Fig. 1).

Regarding claim 2, Sandhu discloses distributed computer networks/enterprise-wide systems (p. 106, ¶4).

Regarding claim 4, Sandhu discloses UP-Roles, containing both abstracted abilities and permissions (p. 122, §5). If a new role is to be created, the next layer (abilities/users) is drilled to/accessed to combine the necessary elements.

Claim Rejections - 35 USC § 103

16. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

17. Claims 5-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Sandhu**, as applied to claim 1 above, in further view of “Issues in the Design of Secure Authorization Service for Distributed Applications” by Varadharajan, Pato and Crall (**Crall**).

Regarding claim 5, Sandhu discloses a system, as described above, but lacks a graphical user interface. However, Crall teaches that a graphical user interface makes it easy for administrators to manage large numbers of users with consistent policies across applications (p. 874). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a graphical user interface to define the security policy. One of ordinary skill in the art would have been motivated to perform such a modification to make it easy for administrators to manage large numbers of users with consistent policies across applications, as taught by Crall (p. 874).

Regarding claim 6-8, Sandhu discloses a plurality of security mechanisms/permissions, a plurality of semantic layers (UP-Roles, abilities, permissions) (p. 122, §5), wherein the first semantic layer combines keys/abilities, wherein each key encapsulates security mechanism application specific information for a security mechanism (permissions for resources) (p. 122, §5), wherein in multiple layers, keys are combined into key chains and exported to another semantic layer (permissions combined into abilities, abilities combined into additional abilities,

combination abilities combined into UP-Roles). Sandhu lacks an explicit translator for translating the security policy to the security mechanisms and lacks a user interface. However, Crall discloses an “Authorization Server”, which employs an interface to make it easy for administrators to manage users (p. 874). In disclosing the physical implementation that Sandhu lacks, Crall further discloses that authorization checks result from the security mechanisms/authorization mechanisms (p. 876, §2.4) when changes are made, translation occurs to keep the authorization database up to date (p. 878, ¶1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a translator to translate the security policy to the security mechanisms and to include a user interface. One of ordinary skill in the art would have been motivated to perform such a modification to implement Sandhu’s invention, in order to keep the authorization database up to date and to allow administrators to manage large groups of users, as taught by Crall (p. 874, p. 876, §2.4 & p. 878, ¶1).

Regarding claim 9, Sandhu discloses the semantic layers (role hierarchy) organized in a POSET/partial order to facilitate inheritance.

Regarding claim 10, Sandhu discloses that new key chains/abilities can be formed by any combinations of abilities and permissions (p. 122, §5), but lacks a user interface. However, Crall teaches that a graphical user interface makes it easy for administrators to manage large numbers of users with consistent policies across applications (p. 874). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a graphical user interface to define the security policy. One of ordinary skill in the art would have

been motivated to perform such a modification to make it easy for administrators to manage large numbers of users with consistent policies across applications, as taught by Crall (p. 874).

Regarding claims 11 & 13, Sandhu discloses a model comprising one or more semantic layers/roles for defining different security policies (p. 122, §5) and constraints (p. 108, ¶1) for each type of user, but lacks a tool for manipulating the model and lacks a translator for translating security policies from the model to security mechanisms in one or more computer resources. However, Crall discloses an “Authorization Server”, which employs an interface to make it easy for administrators to manage users (p. 874). In disclosing the physical implementation that Sandhu lacks, Crall further discloses that authorization checks result from the security mechanisms/authorization mechanisms (p. 876, §2.4) when changes are made, translation occurs to keep the authorization database up to date (p. 878, ¶1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a translator to translate the security policy to the security mechanisms and to include a tool for manipulating the model. One of ordinary skill in the art would have been motivated to perform such a modification to implement Sandhu’s invention, in order to keep the authorization database up to date and to allow administrators to manage large groups of users, as taught by Crall (p. 874, p. 876, §2.4 & p. 878, ¶1). As modified, Sandhu discloses enabling an administrator to encapsulate security mechanism application specific information for each security mechanism, wherein encapsulating includes forming a key/permission for each security mechanism/permission, combine keys to form key chains/abilities, encapsulate key chains/abilities as keys/abilities within two or more semantic layers (abilities, UP-roles), pass the key chain keys/abilities to other semantic layers (abilities->abilities, abilities->UP-roles, UP-

roles->UP-roles), form user key chains/UP-roles from the key chain keys, and associate users with user key chains (UP-roles designated) (p. 122).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis-Jacques can be reached on (571) 272-6962. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MJS



August 1, 2006



JACQUES LOUIS JACQUES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100